



Security architecture establishment and mobility management for information networks

著者	李 睿棟
内容記述	Thesis (Ph. D. in Engineering)--University of Tsukuba, (A), no. 4635, 2008.3.25 Includes bibliographical references (leaves 159-172)
発行年	2008
URL	http://hdl.handle.net/2241/111003

氏 名 (国籍)	李 睿 棟 (中 国)
学 位 の 種 類	博 士 (工 学)
学 位 記 番 号	博 甲 第 4635 号
学位授与年月日	平成 20 年 3 月 25 日
学位授与の要件	学位規則第 4 条第 1 項該当
審 査 研 究 科	システム情報工学研究科
学 位 論 文 題 目	Security Architecture Establishment and Mobility Management for Information Networks (情報ネットワークにおけるセキュリティ・アーキテクチャーの確立とモビリティ・マネジメントに関する研究)
主 査	筑波大学教授 博士 (工学) 李 韻
副 査	筑波大学教授 工学博士 海老原 義 彦
副 査	筑波大学教授 工学博士 岡 本 栄 司
副 査	筑波大学教授 博士 (理学) 加 藤 和 彦
副 査	筑波大学准教授 博士 (情報科学) 木 村 成 伴
副 査	筑波大学准教授 博士 (工学) 満 保 雅 浩

論 文 の 内 容 の 要 旨

本論文では、セキュリティと性能の観点から、情報ネットワークにおけるセキュリティアーキテクチャーと移動性管理に関する研究を行っている。本論文の第 1 章で研究の背景と位置付けを述べている。第 2 章でモバイルアドホックネットワークにおけるセキュリティアーキテクチャーについて概説している。第 3 章でモバイルアドホックネットワークにおけるセキュア通信のための既存の鍵管理方式を紹介し、その問題点を指摘している。そして、各ノードが行う局所公開鍵管理方式を新たに提案し、シミュレーションにより、提案方式の有効性を示している。第 4 章でモバイルアドホックネットワークの信用管理 (Trust Management) 方式を論じている。既存の Reputation-based 方式と Trust Establishment 方式の問題点を指摘し、直接の観察情報と間接情報を用いる客観的信用管理方式を新たに提案している。また、評価を行い、提案した方式が既存の方式より有効であることを示している。第 5 章と第 6 章でグループ通信におけるマルチキャストの鍵管理について研究を行っている。まず関連研究を概説し、既存のマルチキャストの鍵管理方式における性能上の問題点を指摘している。そして、メモリと通信の負荷が少ない分散鍵管理方式を新たに提案し、その有効性を確認している。第 7 章と第 8 章では、次世代モバイル IPv6 におけるハンドオフ管理方式について研究を行っている。まず、広く使われている既存の Fast Handover 管理方式を概説し、その問題点を指摘している。そして、位置登録更新を先に行う Enhanced Fast Handover 方式を新たに提案し、その有効性を示している。最後に、第 9 章で論文をまとめ、今後の課題について述べている。

審 査 の 結 果 の 要 旨

本論文では、セキュリティと性能の観点から、情報ネットワークにおけるセキュリティアーキテクチャーと移動性管理に関する研究を行っている。具体的には、モバイルアドホックネットワークにおける鍵管理方式と信用管理方式、グループ通信におけるマルチキャストのアクセス制御、モバイル IPv6 におけるハンドオフ管理方式に関する 4 つの研究問題を取り上げ、それぞれに対して新たな方式を提案している。また、シミュレーション実験と解析手法により、提案した方式の有効性を確認している。これらの研究は情報工学上貢献するところが大きいと判断される。今後は、提案した方式を実情報ネットワークシステム上に実装し、より現実的なネットワーク環境でその有効性を示すことが望まれる。

よって、著者は博士（工学）の学位を受けるに十分な資格を有するものと認める。